



OSINT + ARCO + PROTECCIÓN DE DATOS

# MAPA-RD: Exposición y Ruta de Cierre

---

Así se ve tu entorno digital desde fuera. Esto es lo que hay que cerrar primero.

MAPA-RD identifica exposición real (visible públicamente), prioriza riesgos y entrega una ruta de cierre ejecutable. Incluye base operativa para gestión ARCO y un esquema mensual de control continuo.

Sin auditorías genéricas. Sin promesas vacías.

**ACME Corp · Reporte RPT-2026-001 · 2026-01-11**

Executive Security Report · Exposición pública · Confidencial

# Índice de Riesgo Digital



Evaluado a partir de 3 vectores de vulnerabilidad

FECHA DE EVALUACIÓN: 2026-01-11

VECTORES DE VULNERABILIDAD

VEC-001	Exposed Database Credentials		85 <small>MÁXIMO</small>
ACTIVO: Production Database (AWS RDS)		TIPO: Cloud Infrastructure	EXPOSICIÓN: Public Repo Leak
<b>DESCRIPCIÓN DEL EVENTO</b>  Hardcoded credentials for the primary production database were identified in a public GitHub repository (config.js). Determining access logs confirmed unauthorized clone events.		<b>RUTA DE CIERRE</b>  <ol style="list-style-type: none"><li>Revoke the exposed AWS IAM credentials immediately.</li><li>Rotate the database master password.</li><li>Audit CloudTrail logs for suspicious activities since the commit date.</li><li>Implement git-secrets to prevent future commits.</li></ol>	
<b>IMPACTO</b> <ul style="list-style-type: none"><li>Full compromise of customer data (PII).</li><li>Potential total service disruption (Ransomware).</li><li>Severe regulatory fines (GDPR/CCPA).</li></ul>			

VEC-002

## Admin Portal without MFA

60 CRÍTICO

ACTIVO:  
admin.acme.com

TIPO:  
Web Application

EXPOSICIÓN:  
Missing Control

### DESCRIPCIÓN DEL EVENTO

The administrative panel allows single-factor authentication. Brute-force attacks or credential stuffing could easily compromise an admin account.

### IMPACTO

- Unauthorized administrative access.
- Data manipulation or deletion.
- Backdoor installation.

### RUTA DE CIERRE

1. Enforce MFA (Time-based OTP) for all admin roles.
2. Restrict access to VPN or trusted IPs only.
3. Implement rate-limiting on the login endpoint.

VEC-003

## Outdated SSL Certificate

35 MEDIO

ACTIVO:  
dev.acme.com

TIPO:  
Dev Environment

EXPOSICIÓN:  
Configuration

### DESCRIPCIÓN DEL EVENTO

The SSL certificate for the development environment is expired, triggering browser warnings and exposing traffic to interception.

### IMPACTO

- Developer workflow disruption.
- Man-in-the-Middle (MitM) risk if used externally.
- Loss of trust validation.

### RUTA DE CIERRE

1. Provision a new LetsEncrypt certificate.
2. Automate renewal via Certbot.